

CLAIMS

What is claimed is:

- 1 1. A method for preventing writes to critical files, comprising:
  - 2 (a) identifying factors associated with a computer;
  - 3 (b) monitoring requests to write to files on the computer; and
  - 4 (c) conditionally preventing the writes to the files on the computer based on the
  - 5 factors to prevent virus proliferation;
  - 6 (d) wherein the factors are altered based on the monitoring of the requests.
- 1 2. The method as recited in claim 1, wherein the factors are selected from the group
- 2 consisting of critical files, critical file locations, and trusted applications.
- 1 3. The method as recited in claim 1, wherein the factors are user configurable.
- 1 4. The method as recited in claim 1, wherein the factors are identified in a registry.
- 1 5. The method as recited in claim 2, wherein the factors include critical files
- 2 associated with an operating system of the computer.
- 1 6. The method as recited in claim 2, wherein the factors include critical file
- 2 locations associated with an operating system of the computer.
- 1 7. The method as recited in claim 6, wherein the critical file locations include
- 2 folders.

- 1 8. The method as recited in claim 2, wherein the factors include trusted  
2 applications that initiate the requests.
- 1 9. The method as recited in claim 1, wherein the factors are updated based on a  
2 user request.
- 1 10. The method as recited in claim 1, wherein the factors are updated from a remote  
2 location via a network.
- 1 11. The method as recited in claim 1, wherein the factors are updated based on the  
2 requests.
- 1 12. The method as recited in claim 1, and further comprising conditionally  
2 preventing the writes to the files on the computer based on a user confirmation.
- 1 13. The method as recited in claim 12, wherein the factors are updated based on the  
2 user confirmation.
- 1 14. A computer program product for preventing writes to critical files, comprising:  
2 (a) computer code for identifying factors associated with a computer;  
3 (b) computer code for monitoring requests to write to files on the computer; and  
4 (c) computer code for conditionally preventing the writes to the files on the  
5 computer based on the factors to prevent virus proliferation;  
6 (d) wherein the factors are altered based on the monitoring of the requests.
- 1 15. The computer program product as recited in claim 14, wherein the factors are  
2 selected from the group consisting of critical files, critical file locations, and  
3 trusted applications.

1 16. The computer program product as recited in claim 14, wherein the factors are  
2 user configurable.

1 17. The computer program product as recited in claim 14, wherein the factors are  
2 identified in a registry.

1 18. The computer program product as recited in claim 15, wherein the factors  
2 include critical files associated with an operating system of the computer.

1 19. The computer program product as recited in claim 15, wherein the factors  
2 include critical file locations associated with an operating system of the  
3 computer.

1 20. The computer program product as recited in claim 19, wherein the critical file  
2 locations include folders.

1 21. The computer program product as recited in claim 15, wherein the factors  
2 include trusted applications that initiate the requests.

1 22. The computer program product as recited in claim 14, wherein the factors are  
2 updated based on a user request.

1 23. The computer program product as recited in claim 14, wherein the factors are  
2 updated from a remote location via a network.

1 24. The computer program product as recited in claim 14, wherein the factors are  
2 updated based on the requests.

1 25. The computer program product as recited in claim 14, and further comprising  
2 computer code for conditionally preventing the writes to the files on the  
3 computer based on a user confirmation.

1 26. The computer program product as recited in claim 25, wherein the factors are  
2 updated based on the user confirmation.

1 27. A system for preventing writes to critical files, comprising:

2 (a) logic for identifying factors associated with a computer;

3 (b) logic for monitoring requests to write to files on the computer; and

4 (c) logic for conditionally preventing the writes to the files on the computer based  
5 on the factors to prevent virus proliferation;

6 (d) wherein the factors are altered based on the monitoring of the requests.

1 28. A method for preventing writes to critical files, comprising:

2 (a) identifying an operating system associated with a computer;

3 (b) looking up at least one of critical files and critical file locations associated with  
4 the operating system; and

5 (c) preventing access to the at least one of critical files and critical file locations  
6 associated with the operating system to prevent virus proliferation.

1 29. A method for preventing virus proliferation, comprising:

2 (a) identifying an operating system;

3 (b) looking up critical files and critical file locations associated with the operating  
4 system;

5 (c) identifying additional critical files and critical file locations in a registry;

6 (d) identifying a plurality of trusted applications;

- 7 (e) storing the critical files, critical file locations, and trusted applications in a
- 8 database;
- 9 (f) altering the database of critical files, critical file locations, and trusted
- 10 applications based on a user request;
- 11 (g) updating the database of critical files, critical file locations, and trusted
- 12 applications based on a remote update via a network;
- 13 (h) receiving a write request;
- 14 (i) determining whether the write request is attempting to write to one of the critical
- 15 file locations in the database;
- 16 (j) if the write request is not attempting to write to one of the critical file locations
- 17 in the database, permitting the write request;
- 18 (k) identifying an application that initiated the write request;
- 19 (l) determining whether the application is one of the trusted applications in the
- 20 database;
- 21 (k) if the application is not one of the trusted applications in the database:
- 22 (i) alerting a user of the write request and of the application that initiated the
- 23 write request,
- 24 (ii) prompting the user to confirm the write request,
- 25 (iii) if the user confirms the write request, prompting the user to confirm the
- 26 write request for future write requests initiated by the application, and
- 27 (iv) if the user does confirm the write request for future write requests
- 28 initiated by the application, adding the application to the database as one
- 29 of the trusted applications;
- 30 (m) identifying a file associated with the write request;
- 31 (n) determining whether the write request is attempting to write to one of the critical
- 32 files in the database;
- 33 (o) if the write request is attempting to write to one of the critical files in the
- 34 database:

- 35 (i) alerting the user of the write request and of the critical file associated
- 36 with the write request,
- 37 (ii) prompting the user to confirm the write request,
- 38 (iii) if the user confirms the write request, prompting the user to confirm the
- 39 write request for future write requests associated with the critical file,
- 40 and
- 41 (iv) if the user does confirm the write request for future write requests
- 42 associated with the critical file, removing the critical file from the
- 43 database; and
- 44 (p) if the application is one of the trusted applications in the database and if the
- 45 write request is not attempting to write to one of the critical files in the database,
- 46 permitting the write request.